



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

Am

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/676,748	09/29/2000	Andrew Edward Nunns	9219-4	2283

20792 7590 06/09/2005

MYERS BIGEL SIBLEY & SAJOVEC
PO BOX 37428
RALEIGH, NC 27627

EXAMINER

NOBAHAR, ABDULHAKIM

ART UNIT PAPER NUMBER

2132.

DATE MAILED: 06/09/2005

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary

Application No.

09/676,748

Applicant(s)

NUNNS, ANDREW EDWARD

Examiner

Abdulahkim Nobahar

Art Unit

2132

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

- 1) ☒ Responsive to communication(s) filed on 16 September 2004.
- 2a) ☒ This action is **FINAL**. 2b) ☐ This action is non-final.
- 3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

- 4) ☒ Claim(s) 1-50 is/are pending in the application.
- 4a) Of the above claim(s) _____ is/are withdrawn from consideration.
- 5) ☐ Claim(s) _____ is/are allowed.
- 6) ☒ Claim(s) 1-50 is/are rejected.
- 7) ☐ Claim(s) _____ is/are objected to.
- 8) ☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

- 9) ☐ The specification is objected to by the Examiner.
- 10) ☐ The drawing(s) filed on _____ is/are: a) ☐ accepted or b) ☐ objected to by the Examiner.
Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).
Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

- 12) ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
- a) ☐ All b) ☐ Some * c) ☐ None of:
1. ☐ Certified copies of the priority documents have been received.
2. ☐ Certified copies of the priority documents have been received in Application No. _____.
3. ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

- 1) ☒ Notice of References Cited (PTO-892)
- 2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
- 3) ☐ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08)
Paper No(s)/Mail Date _____
- 4) ☐ Interview Summary (PTO-413)
Paper No(s)/Mail Date. _____
- 5) ☐ Notice of Informal Patent Application (PTO-152)
- 6) ☐ Other: _____

ps

Response to Arguments

1. This communication is in response to applicants' response received on September 09, 2004.
2. The amendments of claims 1, 4, 6, 9, 13, 14, 16, 19, 21, 24-29, 32-35, and 37-47 are acknowledged.
3. Applicant's arguments have been fully considered and are persuasive. Therefore, the rejection has been withdrawn. However, applicants' amendments have necessitated a new search. A new grounds of rejection based on newly discovered prior art follow below.

Claim Rejections - 35 USC § 112

The following is a quotation of the first paragraph of 35 U.S.C. 112:

The specification shall contain a written description of the invention, and of the manner and process of making and using it, in such full, clear, concise, and exact terms as to enable any person skilled in the art to which it pertains, or with which it is most nearly connected, to make and use the same and shall set forth the best mode contemplated by the inventor of carrying out his invention.

Claims 1, 6, 9, 13, 16, 19, 21, 24, 26, 29, 32, 34, 35, 37, 43 and 44 are rejected under 35 U.S.C. 112, first paragraph, as failing to comply with the written description requirement. The claim(s) contains subject matter, which was not described in the specification in such a way as to reasonably convey to one skilled in the relevant art that the inventor(s), at the time the application was filed, had possession of the claimed invention.

Claims 1, 6, 9, 13, 16, 19, 21, 24, 26, 29, 32, 34, 35, 37, 43 and 44 recite "during ... a first time interval". The specification does not describe that how many "time intervals" exist during the period of operation of a programmable logic device and when the recited "first time interval" starts and when it ends. Applicant has not correlated this issue with any part of the specification in the response to the previous office action. Appropriate correction is required.

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negated by the manner in which the invention was made.

Claims 1-3, 11, 16, 18, 21, 23, 26, 32, 33, 37-41 and 44 are rejected under 35 U.S.C. 103(a) as being unpatentable over Priem et al. (5,652,793; hereinafter Priem) in view of Thompson et al (5,267,312; hereinafter Thompson).

Referring to claims 1, Priem discloses a method and apparatus for controlling the operation of a computer system (corresponding to the recited programmable logic device) (col. 2, line 59-col. 3, line 10). Priem also discloses an encoding circuit (corresponding to the recited integrated circuit) that generates a verification value

Art Unit: 2132

(corresponding to the recited a second encrypted data stream) by using a secret key to encode a concatenated value. The concatenated value is produced from concatenating an application identifier (corresponding to the recited a first data stream) and a secret plaintext value (col. 4, lines 38-44). Priem further discloses that the verification value is sent to a comparison circuit (corresponding to the recited authorization device) to be compared with a password whether to allow the software to be run on the computer system (col. 4, lines 44-52). This comparison is performed (col. 2, lines 5-10 and col. 4, lines 27-37) at intervals (corresponding to the recited periodically) each time the application program is run (examiner interprets that "during first time interval" means the beginning of running a program). Priem, however, does not expressly disclose that the first and second data streams are time-varying streams during the time interval that a programmable logic device is operating.

Thompson discloses a system that it makes difficult for an unauthorized receiver to descramble pre-scrambled entertainment signals (col. 2, lines 40-67). Thompson discloses that the scrambles signals are transmitted from a head-end to a user receiver that includes a programmable integrated device (PLD) and an authorized mechanism that descrambles the transmitted signals for authorized receivers (Figs. 2A', 4A', 4B' and 4B"; col. 14, lines 48-67; col. 20, lines 1-12; col. 20, lines 13-50). Thompson also discloses that in the process of descrambling the received scrambled entertainment signals in a PLD (see Fig. 4b') the authorizing signal 477 (corresponding to the recited first data stream) is generated from the signal 430** (corresponding to the recited second data stream) (col. 20, lines 51-64). Thompson further discloses that a local

Art Unit: 2132

control unit 478 based on the generated signal 477 authorizes the switch 472 (Fig. 4B") for allowing the descrambled signals to be displayed (corresponding to the recited to assess whether operation of a PLD is authorized). This process is continued so long as the subscriber box 460 (Fig. 4B') is receiving the signals 441 from a head-end. Thus, the process of authorization of a subscriber box is an ongoing process, which is executed during the time interval of receiving signals. Therefore, the signals 477 and 430** are time-varying signals.

It would have been obvious to a person of ordinary skill in the art at the time the invention was made to implement the continuous authorization process of displaying signals (i.e., operation of a PLD) as taught in Thompson in the method and apparatus of Priem, because it would make difficult to reverse engineer the internal configuration of a PLD (Thompson, col. 14, lines 55-67).

Referring to claims 2, 33, 40 and 41, Thompson discloses the use of a multiplexer that produces time-varying signals from one or more input signals by utilizing time division multiplexing technique (col. 39, line 61-col. 40, line 33).

Referring to claim 3, Priem discloses:

Wherein said integrated circuit component utilizes an encryption operation to generate the second encrypted data stream from the first data stream (col. 3, lines 54-56; col. 5, lines 25-32).

Referring to claim 11, Priem discloses:

Wherein said integrated circuit component utilizes an encryption operation to generate the second encrypted data stream from the first data stream (col. 3, lines 54-56; col. 5, lines 25-32).

Referring to claims 16, 21, 26 and 44, Priem discloses:

An integrated system (see Fig. 1), comprising:

an authorization device that generates a first encrypted data stream (col. 4, lines 3-17, where the password which is an encrypted data stream corresponds to the recited first encrypted data stream);

a programmable logic device that generates a second encrypted data stream while simultaneously operating under at least partial control of configuration data during a first time interval (col. 4, lines 37-44, where the verification value corresponds to the recited second encrypted data stream generated by the an encoding circuit of a computer system corresponding to the recited a programmable logic device and it is interpreted by the examiner that the "during a first time interval" means the beginning of program operation); and

authorization detection circuitry that at least periodically compares the first and second encrypted data streams during the first time interval and disables operation of said programmable logic device if the first and second encrypted data streams indicate that said programmable logic device is not authorized to utilize the configuration data

(col. 4, lines 44-52; Fig. 2, where the comparison circuit corresponds to the recited authorization detection circuitry).

Priem, however, does not expressly disclose that the first and second data streams are time-varying streams during the time interval that a programmable logic device is operating.

Thompson discloses a system that it makes difficult for an unauthorized receiver to descramble pre-scrambled entertainment signals (col. 2, lines 40-67). Thompson discloses that the scrambles signals are transmitted from a head-end to a user receiver that includes a programmable integrated device (PLD) and an authorized mechanism that descrambles the transmitted signals for authorized receivers (Figs. 2A', 4A', 4B' and 4B"; col. 14, lines 48-67; col. 20, lines 1-12; col. 20, lines 13-50). Thompson also discloses that in the process of descrambling the received scrambled entertainment signals in a PLD (see Fig. 4b') the authorizing signal 477 (corresponding to the recited first data stream) is generated from the signal 430** (corresponding to the recited second data stream) (col. 20, lines 51-64). Thompson further discloses that a local control unit 478 based on the generated signal 477 authorizes the switch 472 (Fig. 4B") for allowing the descrambled signals to be displayed (corresponding to the recited to assess whether operation of a PLD is authorized). This process is continued so long as the subscriber box 460 (Fig. 4B') is receiving the signals 441 from a head-end. Thus, the process of authorization of a subscriber box is an ongoing process, which is executed during the time interval of receiving signals. Therefore, the signals 477 and 430** are time-varying signals.

It would have been obvious to a person of ordinary skill in the art at the time the invention was made to implement the continuous authorization process of displaying signals (i.e., operation of a PLD) as taught in Thompson in the method and apparatus of Priem, because it would make difficult to reverse engineer the internal configuration of a PLD (Thompson, col. 14, lines 55-67).

Referring to claim 18 and 23, Priem discloses:

The system of claim 16, wherein said authorization detection circuitry is internal to said programmable logic device (col. 4, lines 44-48, where the comparison circuit 30 corresponds to the recited authorization detection circuitry which is part of the computer system 10 corresponding to the recited programmable logic circuit); wherein said programmable logic device utilizes an encryption operation to generate the second encrypted data stream (see Fig. 2, col. 3, lines 54-56, col. 4, lines 40-44 and col. 5, lines 24-27, where the verification value which is an encrypted data stream is produced by an encryption operation utilized by the circuitry of the computer system corresponding to the recited programmable logic device); and wherein each of a plurality of bits in the second encrypted data stream is determined by evaluating at least one bit in the first encrypted data stream (see Fig. 2, where comparator 30 compares the bit stream of the verification value with the bit stream of the password which is an encrypted data stream).

Referring to claim 32 and 37, Priem discloses:

An authorization device, comprising:

a first integrated circuit component (col. 4, lines 35-37, where the encoding circuit corresponds to the recited first integrated circuit) that in response to a first data stream generated external to said first component (col. 4, lines 33-35, where the application identifier corresponding to the recited a first data stream generated outside the encoding circuit col. 4, lines 3-10) generates a second data stream (col. 4, lines 40-45, the verification value) that is at least periodically evaluated by a distinct second integrated circuit component (col. 4, lines 44-47, where the comparison circuit corresponds to the recited second integrated circuit and the comparison operation is performed at intervals during each time the program is run) to assess whether performance of operations within the second integrated circuit component are authorized during a time interval when the first data stream is being generated (col. 4, lines 46-52, examiner interprets that the recited the second integrated circuit refers to the programmable logic device and the first data stream refers to the data stream being generated in response to received or inputted first data stream). Priem, however, does not expressly disclose that the first and second data streams are time-varying during the time interval that a programmable logic device is operating.

Thompson discloses a system that it makes difficult for an unauthorized receiver to descramble pre-scrambled entertainment signals (col. 2, lines 40-67). Thompson discloses that the scrambles signals are transmitted from a head-end to a user receiver that includes a programmable integrated device (PLD) and an authorized mechanism that descrambles the transmitted signals for authorized receivers (Figs. 2A', 4A', 4B'

Art Unit: 2132

and 4B"; col. 14, lines 48-67; col. 20, lines 1-12; col. 20, lines 13-50). Thompson also discloses that in the process of descrambling the received scrambled entertainment signals in a PLD (see Fig. 4b') the authorizing signal 477 (corresponding to the recited first data stream) is generated from the signal 430** (corresponding to the recited second data stream) (col. 20, lines 51-64). Thompson further discloses that a local control unit 478 based on the generated signal 477 authorizes the switch 472 (Fig. 4B") for allowing the descrambled signals to be displayed (corresponding to the recited to assess whether operation of a PLD is authorized). This process is continued so long as the subscriber box 460 (Fig. 4B') is receiving the signals 441 from a head-end. Thus, the process of authorization of a subscriber box is an ongoing process, which is executed during the time interval of receiving signals. Therefore, the signals 477 and 430** are time-varying signals.

It would have been obvious to a person of ordinary skill in the art at the time the invention was made to implement the continuous authorization process of displaying signals (i.e., operation of a PLD) as taught in Thompson in the method and apparatus of Priem, because it would make difficult to reverse engineer the internal configuration of a PLD (Thompson, col. 14, lines 55-67).

Referring to claim 38, Priem discloses:

The system of claim 37, wherein said second component comprises an integrated circuit selected from the group consisting of ASICs and PLDs (col. 2, lines 1-5; col. 2, line 60-col. 3, 10).

Referring to claim 39, Priem discloses:

The system of claim 37, wherein said second component generates the first data stream (col. 4, lines 37-50, where the encoding circuit generates the encrypted verification value); and wherein said first and second components comprise first and second stream encryptors therein, respectively (col. 4, lines 5-10 and col. 4, lines 40-44).

Claim 4, 5, 12, 14, 15, 17, 22, 25, 27, 28, 42, 45-47 and 50 are rejected under 35 U.S.C. 103(a) as being unpatentable over Priem et al. (5,652,793; hereinafter Priem) in view of Thompson et al (5,267,312; hereinafter Thompson) as applied to claims 1-3, 11, 16, 18, 21, 23, 26, 32, 33, 37-41 and 44 above, and further in view of Folmsbee (6,609,201 B1).

Referring to claims 4, 5, 12 and 42, these claims are rejected as applied to like elements of claim 1 as stated above and further the following:

Priem in view of Thompson discloses a method for authorizing operation of an application program on a computer (corresponding to the programmable logic device) (see Priem, abstract). Priem in view of Thompson, however, does not expressly disclose a circuit to intentionally insert error into the second encrypted data stream.

Folmsbee teaches a CPU (microprocessor) for secure execution of programs that includes a reconfigurable logic circuitry for processing instructions from an instruction buffer included in the microprocessor (col. 2, lines 15-33). Folmsbee further

Art Unit: 2132

teaches a circuitry for generating errors and intentionally inserting into the data encrypted stream (col. 8, line 66-col. 9, line 15; Fig. 3). Folmsbee also teaches a permutation function for producing a data bit stream that is a combination of encrypted codes and other codes such as error correction codes (col. 8, lines 32-44)

It would have been obvious to a person of ordinary skill in the art at the time the invention was made to implement a permutation function and a circuitry to intentionally insert errors into the encrypted data stream as taught in Folmsbee in the method and apparatus of Priem in view of Thompson, because it would provide an encryption scheme which prevents unauthorized persons from "attacking" the encryption of the software through analysis of the input and output of user commands and instruction sets from the software (Folmsbee, col. 2, lines 2-15).

Referring to claims 14, 15, 17, 22, 27 and 45, Priem in view of Thompson discloses a method for authorizing operation of an application program on a computer (corresponding to the programmable logic device) (see Priem, abstract). Priem in view of Thompson as stated above in the rejection of claim 1 that also discloses that a time-varying verification value (corresponding to the recited first encrypted data stream) is generated based on a concatenated plaintext value and an application identifier (corresponding to the recited a first data stream) (Priem, col. 4, lines 37-44). Priem in view of Thompson, however, does not expressly disclose the use of a random number generator to generate random sequence of bits to be used for generation of encrypted data stream.

Folmsbee discloses a random number generator that is configured to produce random sequence of bit stream (col. 9, lines 27-36; col. 11, lines 24-30).

It would have been obvious to a person of ordinary skill in the art at the time the invention was made to implement a random number generator coupled to the integrated circuit to generate random sequence of data stream as taught in Folmsbee in the method and apparatus of Priem in view of Thompson, because it would provide an encryption scheme which prevents unauthorized persons from "attacking" the encryption of the software through analysis of the input and output of user commands and instruction sets from the software (Folmsbee, col. 2, lines 2-15).

Referring to claims 25 and 46, Priem in view of Thompson discloses a method for authorizing operation of an application program on a computer (corresponding to the programmable logic device) (see Priem, abstract). Priem in view of Thompson also discloses that the authenticator including a comparison circuit (corresponding to the recited authorization device) is coupled to the control processor (corresponding to the recited integrated circuit) by a bus (see Priem, Fig. 1). Priem in view, however, does not expressly disclose that the data streams are being time division multiplexed during the process of authorization of the program operation.

Folmsbee teaches a CPU (i.e., microprocessor) for secure execution of programs that includes a reconfigurable logic circuitry for processing instructions from an instruction buffer included in the microprocessor (col. 2, lines 15-33). Folmsbee further

Art Unit: 2132

teaches the use of a multiplexer as a part of the control logic system for multiplexing two streams of data (col. 6, lines 10-35).

It would have been obvious to a person of ordinary skill in the art at the time the invention was made to implement a multiplexer as a part of the programmable logic device (i.e., coupled to the integrated circuit) for time division multiplexing two data streams as taught in Folmsbee in the integrated circuit of Priem in view Thompson computer system, because it would facilitate the control of other functions such as an error correction operation (Folmsbee, col. 6, lines 24-31).

Referring to claims 47 and 50, Priem in view Thompson discloses a method for authorizing operation of an application program on a computer (corresponding to the programmable logic device) (see Priem, abstract). Priem in view Thompson as stated above in the rejection of claim 1 also discloses that an encoding circuit (corresponding to the recited a first integrated circuit) generates a time-varying verification value (corresponding to the recited first encrypted data stream) (Priem, col. 4, lines 37-44). The verification value is produced by encoding (i.e., encrypting) a value obtained from the concatenation of a plaintext value and an application identifier (corresponding to the recited a first data stream) (Priem, col. 4, lines 37-44). Priem in view Thompson further discloses that an encrypted value named password (corresponding to the recited the second data stream) is generated in a separate integrated circuit (corresponding to the recited second integrated circuit) (Priem, col. 4, lines 7-15). Priem in view Thompson,

Art Unit: 2132

however, does not expressly disclose the use of a random number generator to generate random sequence of bits to be used for generation of encrypted data stream.

Folmsbee discloses a random number generator that is configured to produce random sequence of bit stream (col. 9, lines 27-36; col. 11, lines 24-30).

It would have been obvious to a person of ordinary skill in the art at the time the invention was made to implement a random number generator coupled to the integrated circuit to generate random sequence of data stream as taught in Folmsbee in the method and apparatus of Priem in view Thompson, because it would provide an encryption scheme which prevents unauthorized persons from "attacking" the encryption of the software through analysis of the input and output of user commands and instruction sets from the software (Folmsbee, col. 2, lines 2-15).

Referring to claim 28, Priem in view Thompson discloses:

The method of claim 27, wherein the first encrypted data stream is generated internal to the programmable logic device (see Priem, col. 4, lines 37-44, where the verification value is produced inside the computer) and the second encrypted data stream is generated external to the programmable logic device (see Priem, col. 4, lines 20-25, where the password, the second encrypted data stream is generated outside the computer).

Allowable Subject Matter

Claims 6-10, 13, 19, 20, 24, 29-31, 34-36, 43, 48 and 49 would be allowable if rewritten or amended to overcome the rejection(s) under 35 U.S.C. 112, first paragraph, set forth in this office action.

Conclusion

Applicant's amendment necessitated the new ground(s) of rejection presented in this Office action. Accordingly, **THIS ACTION IS MADE FINAL**. See MPEP § 706.07(a). Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire **THREE MONTHS** from the mailing date of this action. In the event a first reply is filed within **TWO MONTHS** of the mailing date of this final action and the advisory action is not mailed until after the end of the **THREE-MONTH** shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than **SIX MONTHS** from the date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Abdulhakim Nobahar whose telephone number is 571-272-3808. The examiner can normally be reached on M-T 8-6.

Art Unit: 2132

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Gilberto Barron can be reached on 571-272-3799. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Abdulkhakim Nobahar
Examiner
Art Unit 2132

an.
AN
June 2, 2005

Gilberto B.
GILBERTO BARRON JR.
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100